RADIUS-Konfiguration mit Cisco Managed Switches der Serien 200 und 300 und Windows Server 2008

Ziel

RADIUS (Remote Authorization Dial-in User Service) bietet eine robuste Möglichkeit zur Benutzerauthentifizierung für den Zugriff auf einen Netzwerkdienst. Aus diesem Grund bieten RADIUS-Server eine zentralisierte Zugriffskontrolle, bei der der Serveradministrator entscheidet, ob ein bestimmtes Segment authentifiziert wird oder nicht. In diesem Artikel werden die allgemeinen Schritte zum Einrichten von RADIUS in einer Client/Server-Umgebung erläutert, in der der Client durch den Cisco Managed Switch der Serien 200/300 repräsentiert wird und auf dem Server Windows Server 2008 mit aktiviertem RADIUS ausgeführt wird.

Unterstützte Geräte

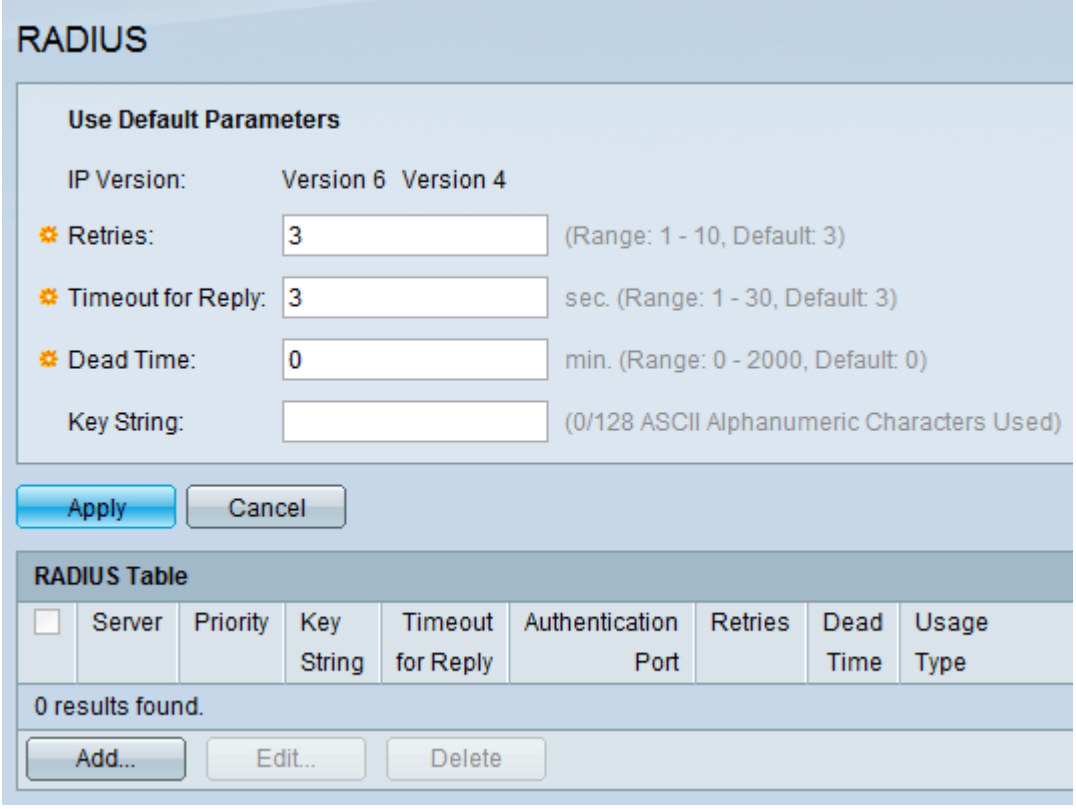
- Cisco Managed Switches der Serien 200 und 300

Schritt-für-Schritt-Anleitung

Die Konfiguration erfolgt in zwei Teilen. Zuerst muss der Switch als RADIUS-Client eingerichtet werden, dann muss der Server korrekt für RADIUS eingerichtet werden.

Einrichten von RADIUS auf dem Switch

Schritt 1: Wählen Sie im Konfigurationsprogramm für die SG200/300 Serie die Option **Security > RADIUS (Sicherheit > RADIUS)**. Die Seite *RADIUS* wird geöffnet:

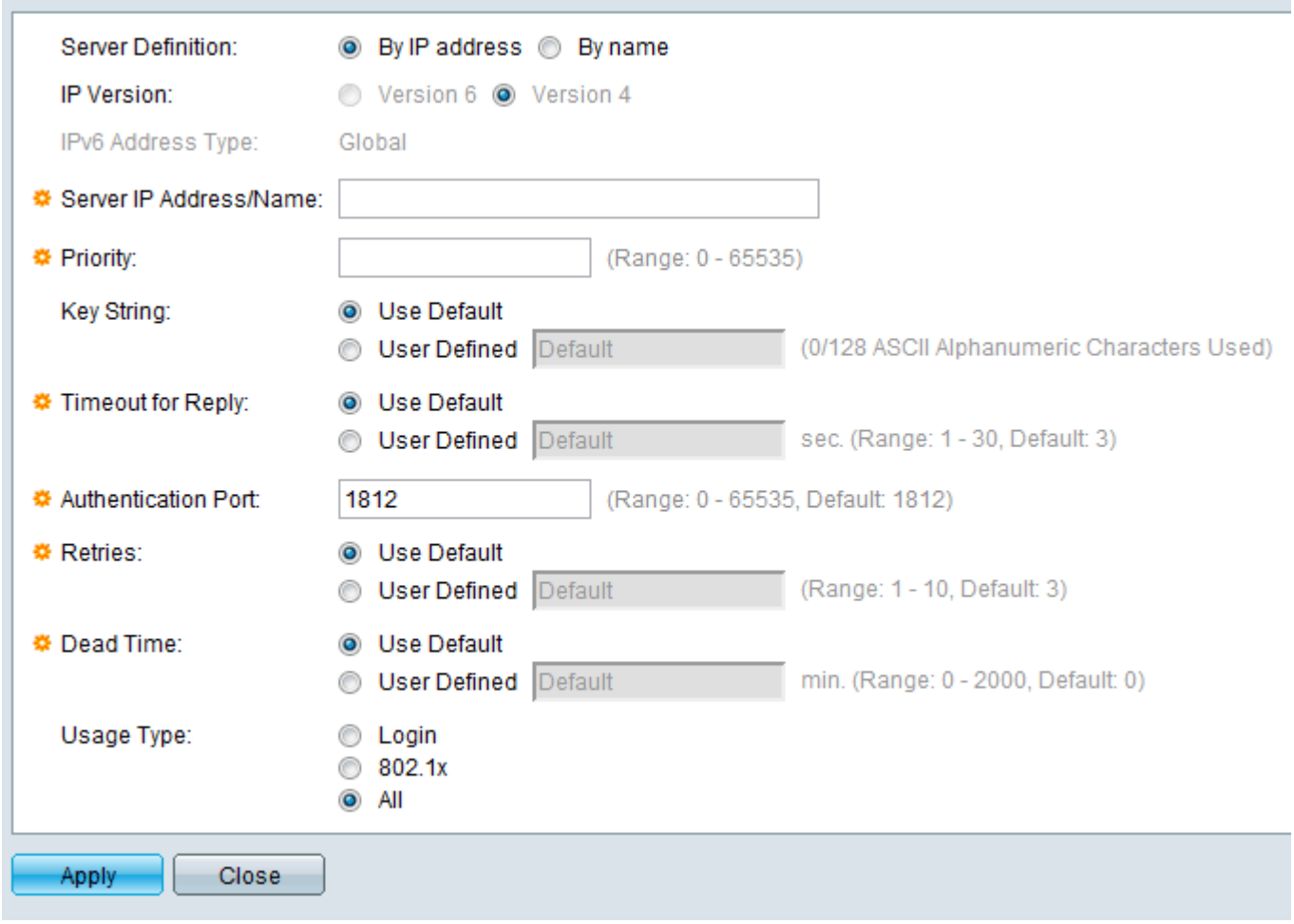


Schritt 2: Geben Sie die RADIUS-Standardeinstellungen ein.

- IP-Version â€" Zeigt die unterstützte IP-Version an.
- Wiederholungen - Geben Sie in diesem Feld die Anzahl der übertragenen Anforderungen ein, die an den RADIUS-Server gesendet werden, bevor ein Fehler auftritt.
- Timeout für Antwort â€" Geben Sie in diesem Feld die Zeit in Sekunden ein, die der Switch auf eine Antwort vom RADIUS-Server wartet, bevor er eine Abfrage erneut versucht.
- Dead Time (Ausfallzeit) - Geben Sie in diesem Feld die Zeit in Minuten ein, die der Switch wartet, bevor er den RADIUS-Server umgeht.
- Schlüsselzeichenfolge - Geben Sie in dieses Feld die Standardzeichenfolge ein, die für die Authentifizierung und Verschlüsselung zwischen dem Switch und dem RADIUS-Server verwendet wird. Der Schlüssel muss mit dem Schlüssel übereinstimmen, der auf dem RADIUS-Server konfiguriert wurde.

Schritt 3: Klicken Sie auf **Apply**, um die aktuelle Konfiguration des Switches mit den RADIUS-Einstellungen zu aktualisieren.

Schritt 4: Sie müssen den RADIUS-Server zum Switch hinzufügen. Klicken Sie auf **Hinzufügen**. Die Seite *RADIUS-Server hinzufügen* wird in einem neuen Fenster geöffnet:



Schritt 5: Geben Sie die Werte in die Felder für den Server ein. Wenn Sie die Standardwerte verwenden möchten, wählen Sie im gewünschten Feld die Option **Standard verwenden**.

- Serverdefinition - In diesem Feld geben Sie an, wie eine Verbindung zum Server hergestellt werden soll, entweder über die IP-Adresse oder den Servernamen.
- IP-Version - Wenn der Server anhand der IP-Adresse identifiziert werden soll, wählen Sie die IPv4- oder die IPv6-Adresse aus.
- IPv6 Address Type (IPv6-Adresstyp): In diesem Feld wird der Typ Global der IPv6-Adresse angezeigt.
- Server-IP-Adresse/-Name â€" Geben Sie in diesem Feld die IP-Adresse oder den Domänennamen des RADIUS-Servers ein.
- Priorität - Geben Sie in diesem Feld die Priorität des Servers ein. Wenn mehr als ein Server konfiguriert ist, versucht der Switch, entsprechend diesem Prioritätswert eine Verbindung zu jedem Server herzustellen.
- Schlüsselzeichenfolge - Geben Sie in dieses Feld die Standardzeichenfolge ein, die für die Authentifizierung und Verschlüsselung zwischen dem Switch und dem RADIUS-Server verwendet wird. Der Schlüssel muss mit dem Schlüssel übereinstimmen, der auf dem RADIUS-Server konfiguriert wurde.
- Timeout für Antwort â€" Geben Sie in diesem Feld die Zeit in Sekunden ein, die der Switch auf eine Antwort vom RADIUS-Server wartet, bevor er eine Abfrage erneut versucht.
- Authentication Port (Authentifizierungsport) - Geben Sie in diesem Feld die UDP-Portnummer ein, die für Authentifizierungsanforderungen für den RADIUS-Server festgelegt wurde.
- Wiederholungen - Geben Sie in diesem Feld die Anzahl der übertragenen Anforderungen ein, die an den RADIUS-Server gesendet werden, bevor ein Fehler auftritt.
- Dead Time (Ausfallzeit) - Geben Sie in diesem Feld die Zeit in Minuten ein, die der Switch wartet, bevor er den RADIUS-Server umgeht.

- Usage Type - Geben Sie in diesem Feld den Authentifizierungstyp des RADIUS-Servers ein. Es gibt drei Optionen:

  - Anmeldung - Der RADIUS-Server authentifiziert Benutzer, die den Switch verwalten möchten.

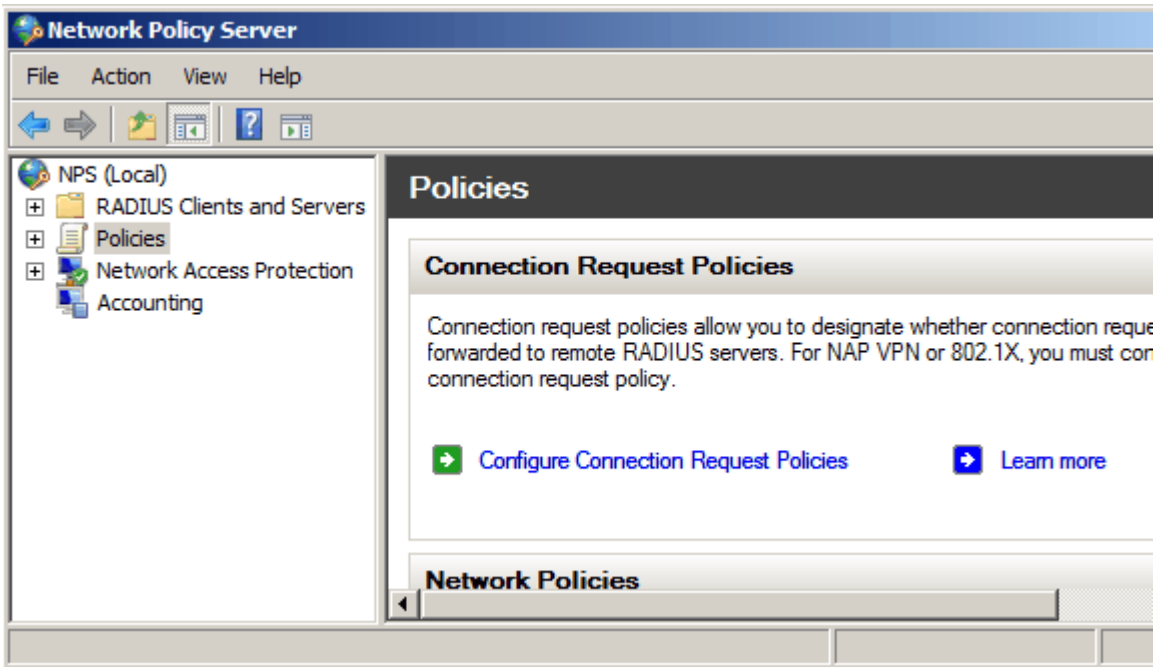
  - 802.1X: RADIUS-Server wird für die 802.1X-Authentifizierung verwendet.

  - Alle - Der RADIUS-Server wird für Anmelde- und 802.1X-Authentifizierungen verwendet.

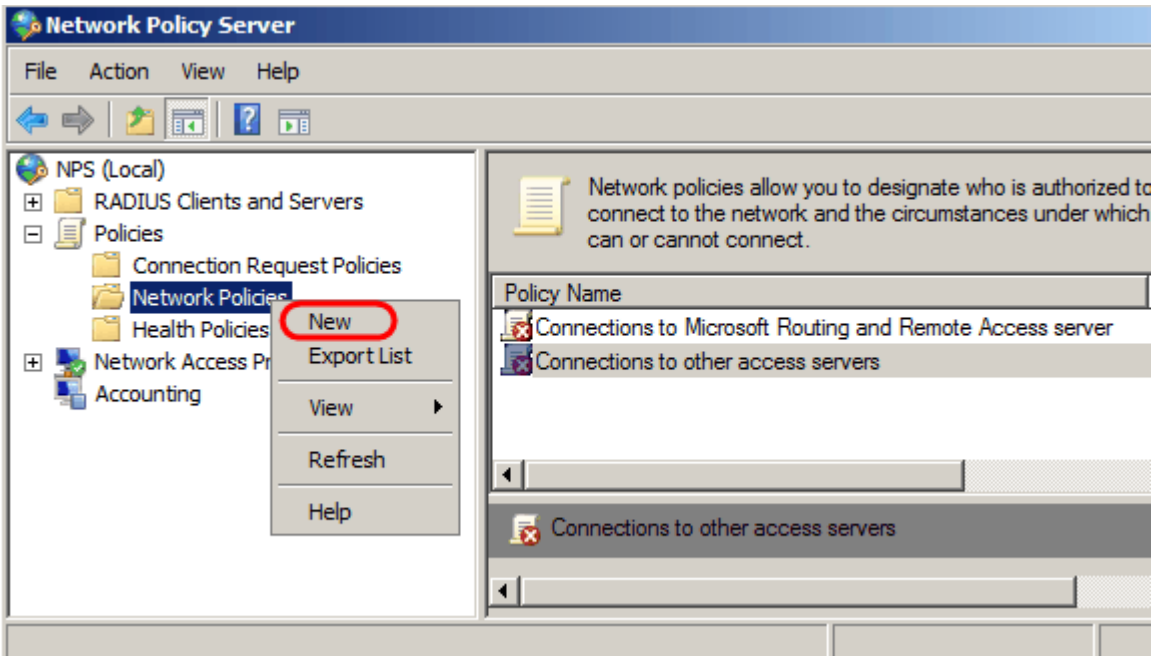
Schritt 6: Klicken Sie auf **Apply**, um die Serverdefinition zur aktuellen Switch-Konfiguration hinzuzufügen.

Konfigurieren von Windows Server 2008 für RADIUS

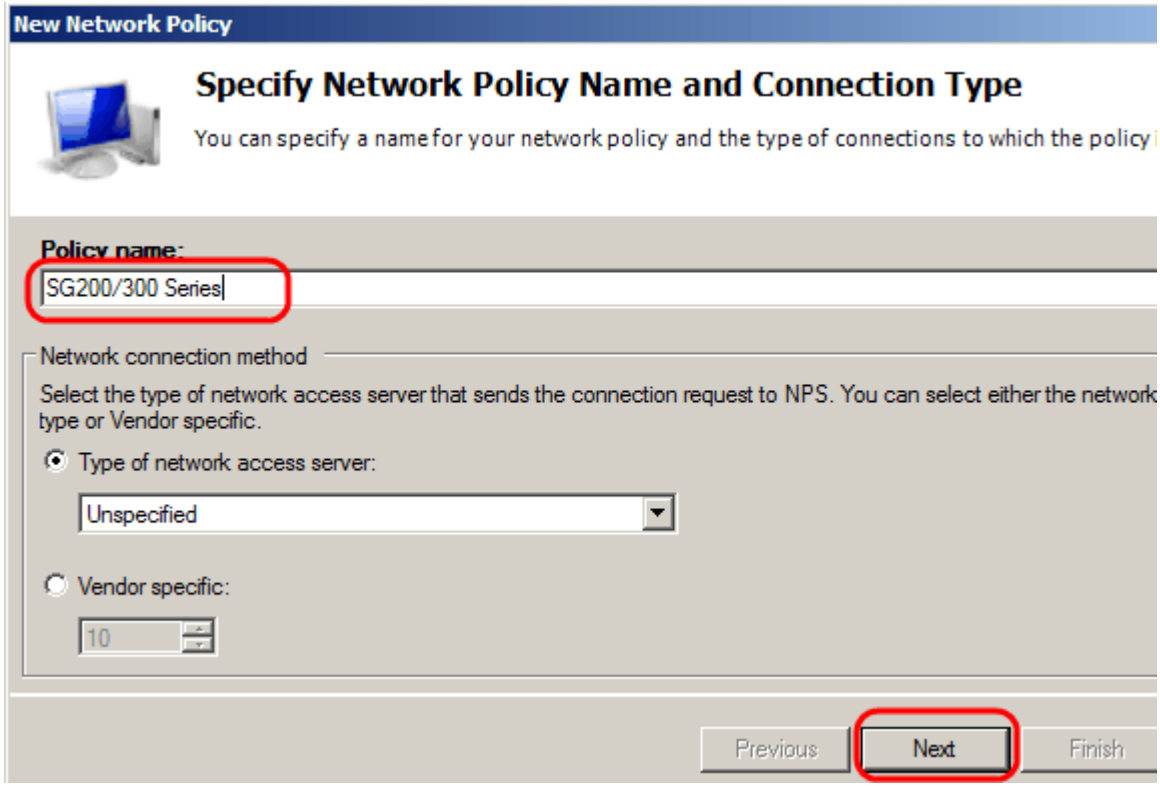
Schritt 1: Wählen Sie auf dem Windows Server 2008-Computer **Start > Verwaltung > Netzwerkrichtlinienserver aus**. Das Fenster *Netzwerkrichtlinienserver* wird geöffnet:



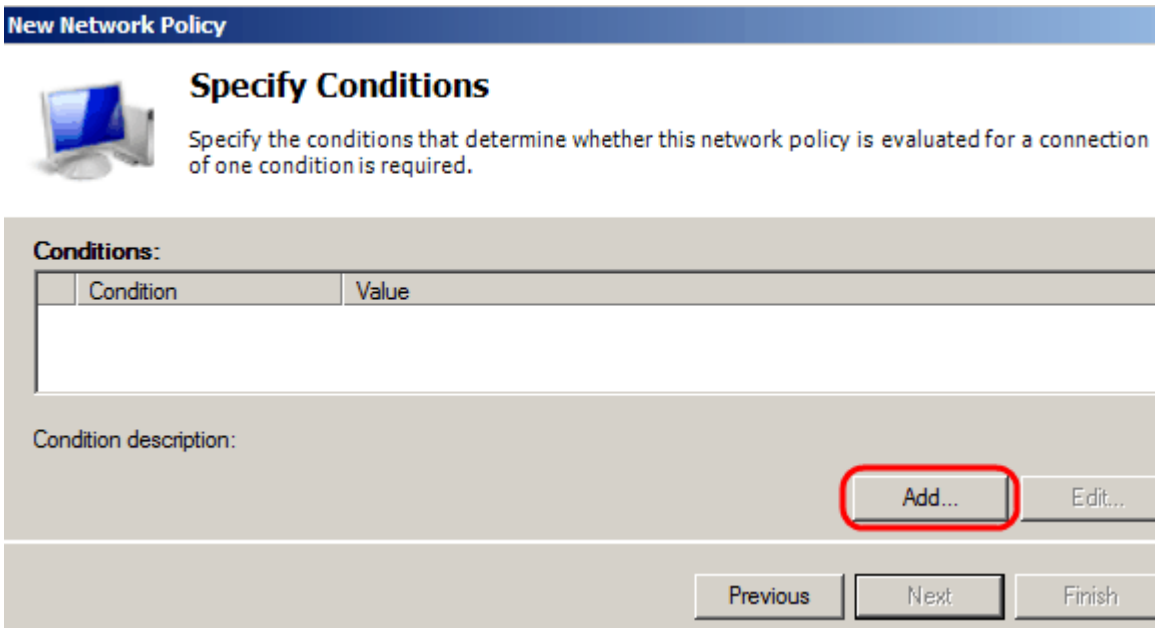
Schritt 2: Um den RADIUS-Server für ein bestimmtes Netzwerksegment zu aktivieren, müssen Sie eine neue Netzwerkrichtlinie erstellen. Um eine neue Netzwerkrichtlinie zu erstellen, wählen Sie **Richtlinien > Netzwerkrichtlinie,** klicken Sie mit der rechten Maustaste, und wählen Sie **Neu aus**. Das Fenster *Neue Netzwerkrichtlinie* wird geöffnet:



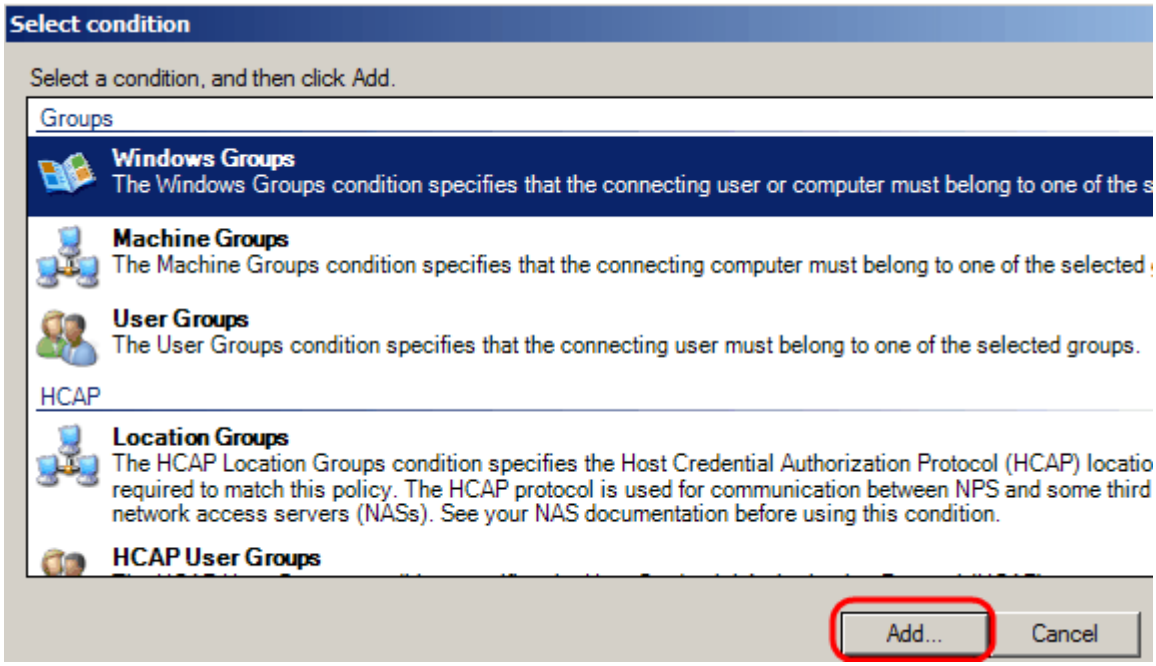
Schritt 3: Geben Sie im Feld Policy Name (Name der Richtlinie) den Namen für die neue Richtlinie ein. Klicken Sie auf **Next** (Weiter).



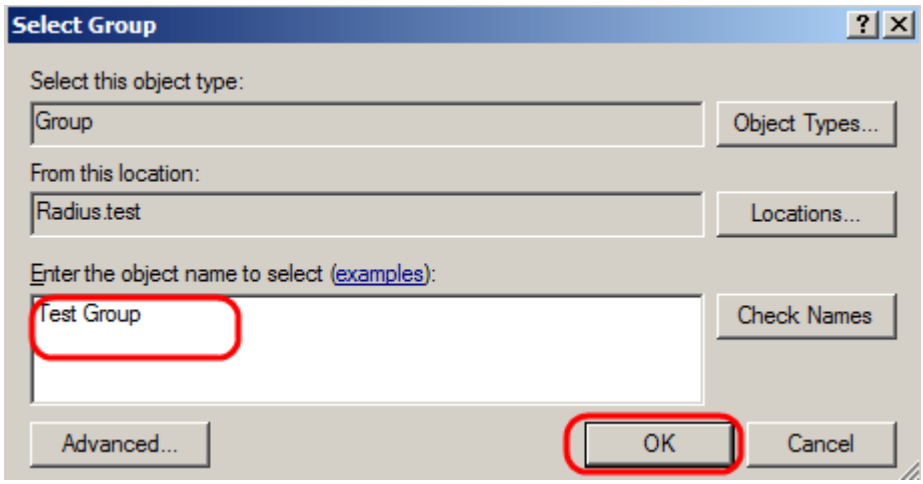
Schritt 4: Sie müssen die Bedingungen dieser Richtlinie angeben. Es müssen zwei Bedingungen erfüllt werden: mit welchem Benutzersegment der RADIUS-Server implementiert wird und mit welcher Methode die Verbindung zu diesem Segment hergestellt wird. Klicken Sie auf **Hinzufügen**, um diese Bedingungen hinzuzufügen.



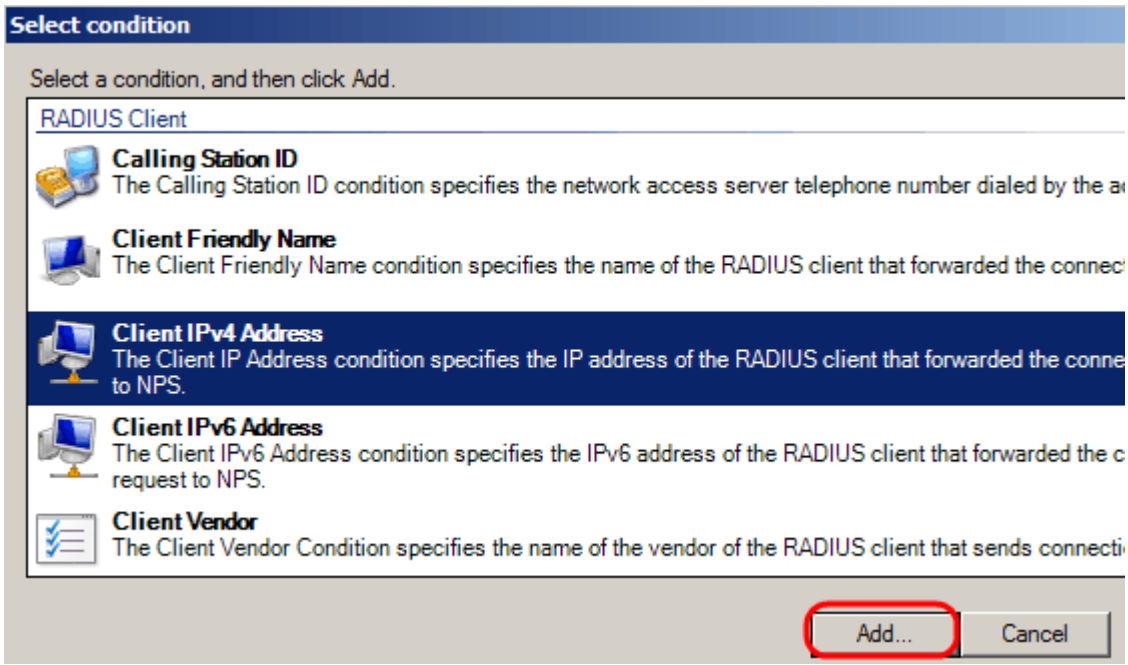
Schritt 5: Unter Gruppen gibt es drei Optionen: Windows-Gruppen, Computergruppen und Benutzergruppen. Wählen Sie die Gruppe entsprechend der Einstellung des Netzwerks aus, und klicken Sie auf **Hinzufügen**. Ein neues Fenster wird geöffnet, das der ausgewählten Gruppe entspricht. Klicken Sie auf **Gruppen hinzufügen**.



Schritt 6: Wählen Sie den Objekttyp und die Position aus, und geben Sie den Namen des Objekts ein. Klicken Sie auf **OK** und dann auf **OK**. Klicken Sie auf **Hinzufügen**, um die nächste Bedingung hinzuzufügen.

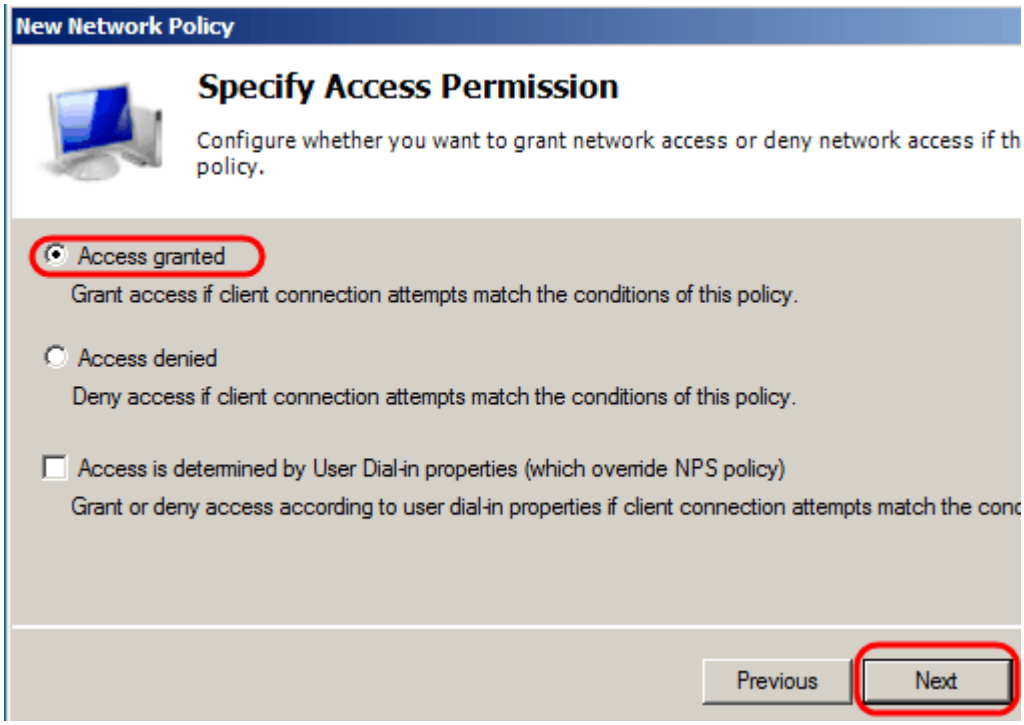


Schritt 7. Wählen Sie unter RADIUS Client (RADIUS-Client) IPv4 Address (IPv4-Adresse) als Methode für die Verbindung des Servers mit den RADIUS-Clients aus, in diesem Fall die IP-Adresse des Switches. Klicken Sie auf **Hinzufügen**.

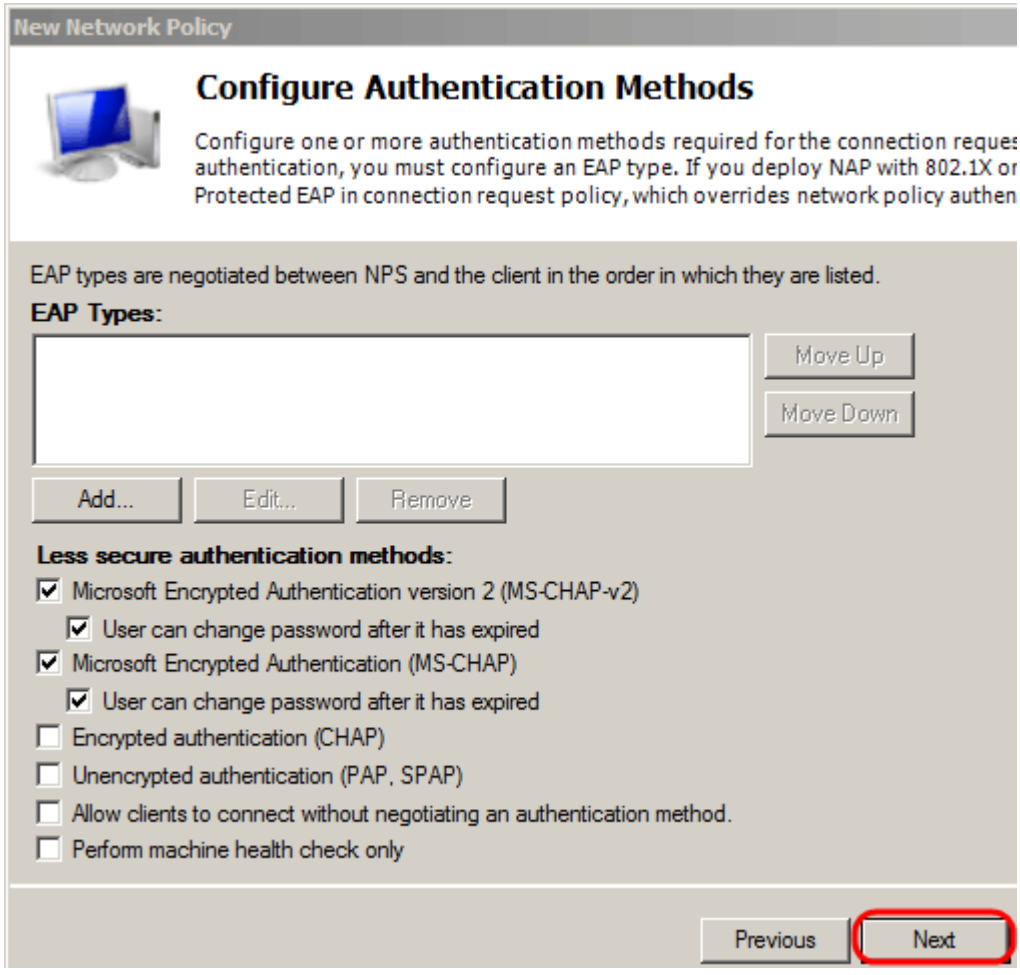


Schritt 8: Geben Sie die entsprechende IP-Adresse ein, und klicken Sie dann auf **OK**. Eine Liste mit den hinzugefügten Bedingungen wird angezeigt. Klicken Sie auf **Weiter**.

Schritt 9. Wählen Sie auf der Seite "Zugriffsberechtigung angeben" die Option **Zugriff gewährt aus**. Klicken Sie auf **Next** (Weiter).



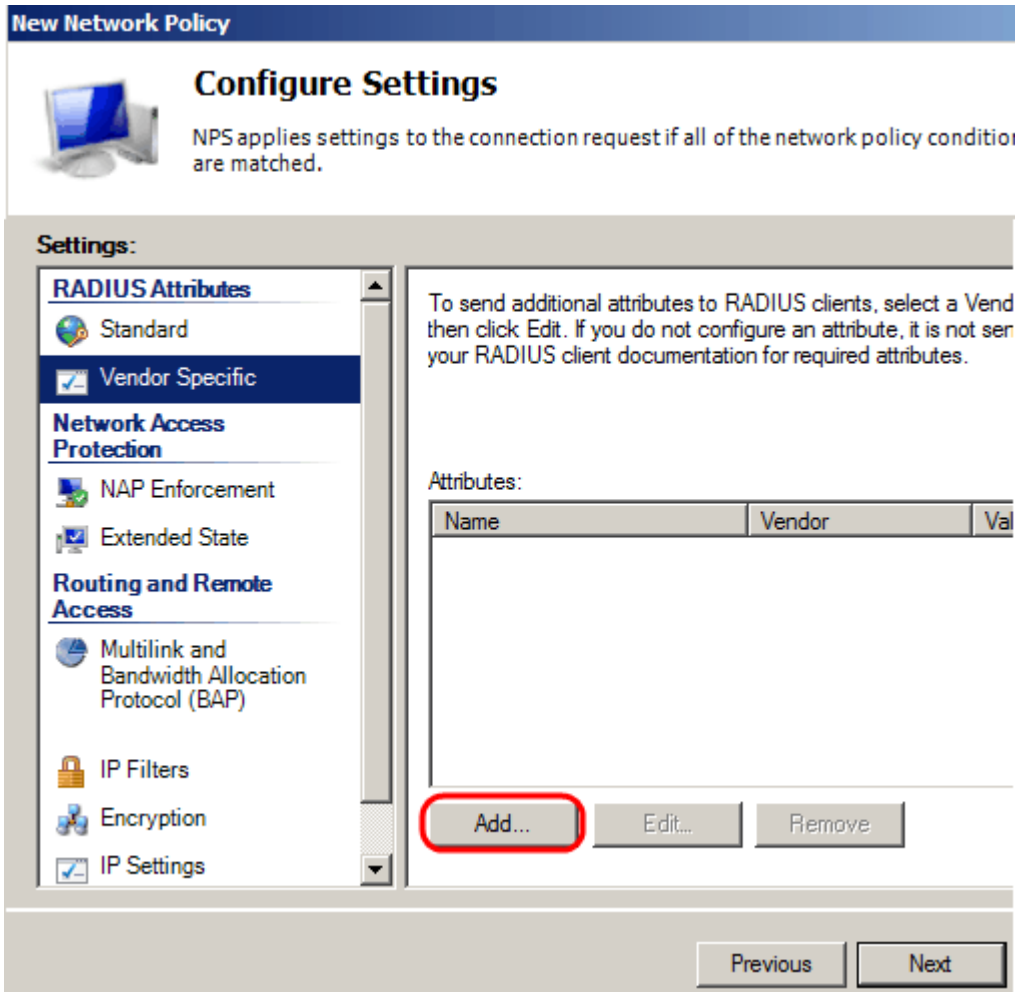
Schritt 10. Legen Sie auf der Authentifizierungsseite die Authentifizierungsmethode fest, die am besten zu Ihrem Netzwerk passt. Klicken Sie auf **Next** (Weiter).



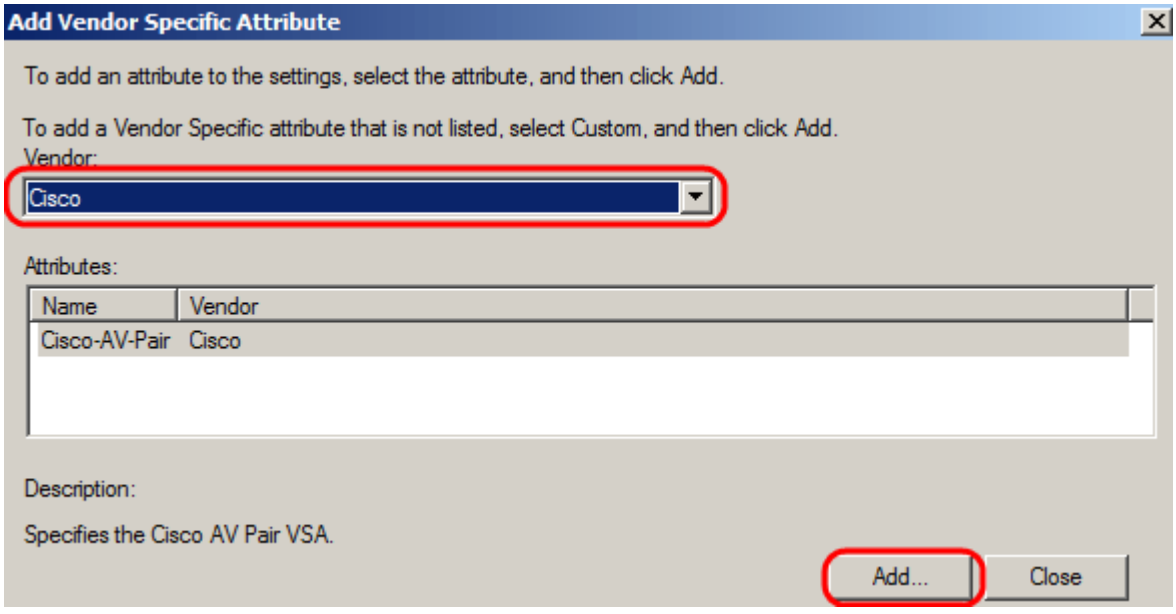
Schritt 11. Verwenden Sie im Fenster Constraints konfigurieren die Standardwerte. Klicken Sie auf **Next** (Weiter).

Schritt 12: Klicken Sie auf der Seite "Configure Settings" unter RADIUS Attributes auf **Vendor Specific**, und klicken Sie dann auf **Add**.

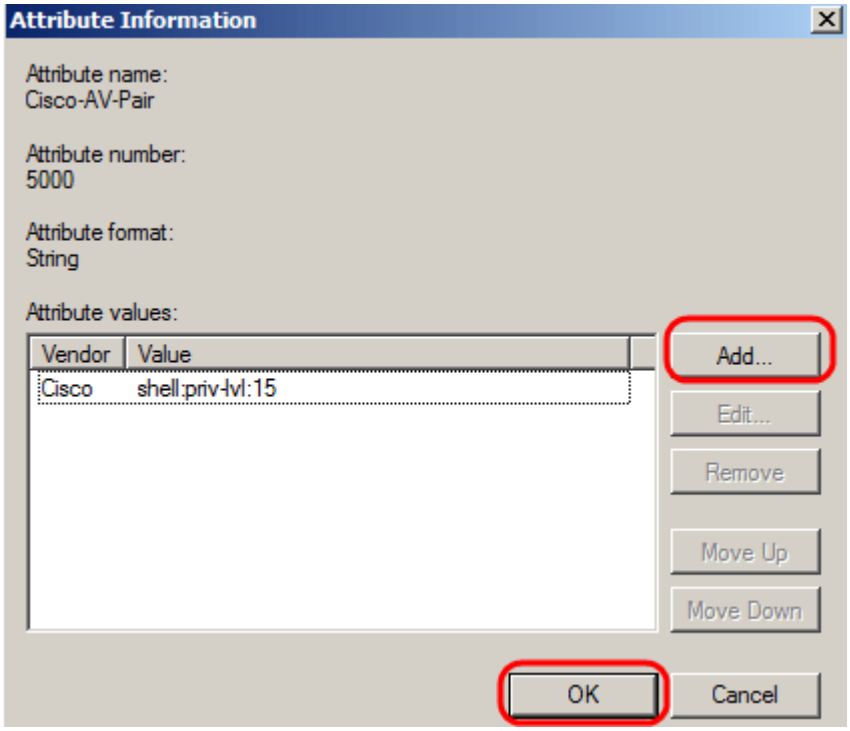
Hinweis: Für die übrigen Einstellungen auf dieser Seite gelten die Standardwerte. Sie müssen sich nur um die anbieterspezifischen Einstellungen kümmern.



Wählen Sie unter Anbieter die Option **Cisco aus**. Klicken Sie auf **Hinzufügen**. Das Fenster *Attributinformationen* wird geöffnet.



Klicken Sie im Fenster Attributinformationen auf **Hinzufügen,** und geben Sie den Wert shell:priv-lvl:15 ein. Klicken Sie auf **OK**.



Hinweis: Dieser Wert wird von Cisco zugewiesen, damit der RADIUS-Server den Zugriff auf das webbasierte Switch-Konfigurationsprogramm gewähren kann.

Klicken Sie auf **OK**, um das Fenster Attributinformationen zu schließen, und klicken Sie dann auf **Schließen**, um das Fenster Herstellerspezifisches Attribut hinzufügen zu schließen. Klicken Sie auf **Next** (Weiter).

Schritt 13: Eine Zusammenfassung der Einstellungen für diese Richtlinie wird angezeigt. Klicken Sie auf **Fertig stellen**. Die Netzwerkrichtlinie wird erstellt.

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

SG200/300 Series

Policy conditions:

Condition	Value
Windows Groups	RADIUS\Test Group
Client IPv4 Address	192.168.1.10

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous | Next | Finish

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.